CLAIM AMENDMENTS

1. (currently amended) ~~A system~~ Apparatus for facilitating digital signing of electronic ~~messages~~ data, said system comprising:

a browser;

coupled to the browser, a signing module; and

coupled to the browser and to the signing module, a signing interface, the signing interface adapted to be invoked by ~~a Web application~~ an executable software program transmitted to the browser from a remote location, and to:

forward data to be signed to the signing module,

receive a digital signature for the data to be signed from the signing module, and

forward the digital signature to a remote location specified by the ~~Web application~~ executable software program.

2. (currently amended) The ~~system~~ apparatus of claim 1, wherein the signing interface comprises a signing interface library having an API, and the ~~Web application~~ executable software program is an applet referenced in a Web page transmitted to the browser from a Web server.

3. (currently amended) The ~~system~~ apparatus of claim 2, wherein the applet is adapted to retrieve the data to be signed from a remote location and to forward the data to be signed to the signing interface.

4. (currently amended) The ~~system~~ apparatus of claim 2, wherein the applet is digitally signed.

5. (currently amended) The ~~system~~ apparatus of claim 1, wherein the signing interface comprises a signing plug-in, and the Web application is a Web page comprising a tag adapted to launch the signing plug-in.

6. (currently amended) The ~~system~~ apparatus of claim 5, wherein the tag is an <EMBED> tag.

7. (currently amended) The ~~system~~ apparatus of claim 5, wherein the tag is an <OBJECT> tag.

8. (currently amended) The ~~system~~ apparatus of claim 1, wherein the data to be signed is retrieved from a remote location specified by the ~~Web Application~~ executable software program.

9. (currently amended) The ~~system~~ apparatus of claim 1, wherein the data to be signed is included in the ~~Web application~~ executable software program.

10. (currently amendedl) The ~~system~~ apparatus of claim 1, wherein the signing module digitally signs the data to be signed with an identity key.

11. (currently amended) The ~~system~~ apparatus of claim 1, wherein the signing module is a smart card subsystem.

12. (currently amended) The ~~system~~ apparatus of claim 1, wherein the digitally signed data includes card and signature security data.

13. (currently amended) The ~~system~~ apparatus of claim 1, wherein the signing interface is obtained from a trusted entity.

14. (currently amended) The ~~system~~ apparatus of claim 13, wherein the signing interface is digitally signed by the trusted entity.

15. (currently amended) The ~~system~~ apparatus of claim 14, wherein the trusted entity is an issuing participant.

16. (currently amended) The ~~system~~ apparatus of claim 1, wherein the signing interface comprises a user interface.

17. (currently amended) The ~~system~~ apparatus of claim 16, wherein the user interface displays the data to be signed to a user, and, prior to the signing interface obtaining the digital signature from the signing module, obtains the user's approval to sign the data.

18. (currently amended) The ~~system~~ apparatus of claim 16, wherein the user interface offers a user ~~the~~ an opportunity to store the data to be signed.

19. (currently amended) The ~~system~~ apparatus of claim 16, wherein the user interface offers a user ~~the~~ an opportunity to view the data to be signed in a software application.

20. (currently amended) The ~~system~~ apparatus of claim 19, wherein the software application is a spreadsheet.

21. (currently amended) A method for facilitating digital signing of electronic ~~messages~~ data, said method comprising the steps of:

a browser~~,~~ receiving an executable software program from a remote location;

~~a signing module,~~

~~and a signing interface, the signing interface adapted to be invoked by a Web application transmitted to the browser from a remote location, the method comprising:~~

~~invoking the~~ the executable software program triggering a signing interface, coupled to the browser, to forward~~ing by the signing interface the~~ data to be signed to ~~the~~ a signing module;

~~receiving at~~ the signing module sending to the signing interface a digital signature for the data to be signed ~~from the signing module~~; and

the signing interface forwarding the digital signature to a remote location specified by the ~~Web application.~~ executable software program.

22. (currently amended) The method of claim 21, wherein the signing interface comprises a signing interface library having an API, and the ~~Web application~~ executable software program is an applet referenced in a Web page transmitted to the browser from a Web server.

23. (original) The method of claim 22, wherein the applet is adapted to retrieve the data to be signed from a remote location and to forward the data to be signed to the signing interface.

24. (original) The method of claim 22, wherein the applet is digitally signed.

25. (currently amended) The method of claim 21, wherein the signing interface comprises a signing plug-in, and the ~~Web application is~~ executable software application comprises a Web page comprising a tag adapted to launch the signing plug-in.

26. (original) The method of claim 25, wherein the tag is an <EMBED> tag.

27. (original) The method of claim 25, wherein the tag is an <OBJECT> tag.

28. (currently amended) The method of claim 21, wherein the data to be signed is retrieved from a remote location specified by the ~~Web application~~ executable software program.

29. (currently amended) The method of claim 21, wherein the data to be signed is included in the ~~Web application~~ executable software program.

30. (original) The method of claim 21, wherein the signing module digitally signs the data to be signed with an identity key.

31. (original) The method of claim 21, wherein the signing module is a smart card subsystem.

32. (original) The method of claim 21, wherein the digitally signed data includes card and signature security data.

33. (original) The method of claim 21, wherein the signing interface is obtained from a trusted entity.

34. (original) The method of claim 33, wherein the signing interface is digitally signed by the trusted entity.

35. (original) The method of claim 34, wherein the trusted entity is an issuing participant.

36. (original) The method of claim 21, wherein the signing interface comprises a user interface.

37. (currently amended) The method of claim 36, wherein, prior to the step of the signing module sending to the signing interface a digital signature, the user interface displays the data to be signed to a user and obtains the user's approval to sign the data.

38. (original) The method of claim 36, wherein the user interface offers a user the opportunity to store the data to be signed.

39. (original) The method of claim 36, wherein the user interface offers a user the opportunity to view the data to be signed in a software application.

40. (original) The method of claim 39, wherein the software application is a spreadsheet.

41. (currently amended) ~~A system~~ Apparatus for facilitating digitally signing data by a first customer, said system comprising:

a browser;

coupled to the browser, a signing module;

coupled to the browser and to the signing module, a signing interface, the signing interface being adapted to facilitate access to system services provided via a four-corner model comprising a root entity, a first participant, a second participant, the first customer, and a second customer, the second customer maintaining a second-customer computer system;

coupled to the browser, means for downloading ~~a Web application~~ an executable software program from the second-customer computer system to the browser;

coupled to the downloading means, means for invoking the signing interface;

coupled to the invoking means, means for determining whether to request a system service;

coupled to the determining means, means for creating a service request for the system service;

coupled to the creating means, means for transmitting the service request;

coupled to the transmitting means, means for receiving a response to the service request;

coupled to the means for receiving a response, means for forwarding the data to be signed to the signing module;

coupled to the forwarding means, means for receiving a digital signature for the data to be signed from the signing module; and

coupled to the means for receiving a digital signature, means for forwarding the digital signature to a remote location specified by the ~~Web application~~ executable software program.

42. (currently amended) The ~~system~~ apparatus of claim 41, ~~further comprising~~ wherein the determining means comprises means for presenting to the first customer an option to request a system service.

43. (currently amended) The ~~system~~ apparatus of claim 42, wherein the system service is a warranty.

44. (currently amended) The ~~system~~ apparatus of claim 43, wherein the response to the service request comprises a warranty, and ~~wherein~~ the warranty is forwarded with the digital signature to the remote location specified by the ~~Web application~~ executable software program.

45. (currently amended) A method for accessing system services provided via a four-corner model, the four corner model comprising:

a root entity~~,~~;

a first participant~~,~~;

a second participant~~,~~;

a first customer, ~~the~~ said first customer being a customer of the first participant, ~~and~~ said first customer maintaining a first-customer computer system, ~~the~~ said first-customer computer system comprising:

a browser,

a signing module,

and a signing interface~~,~~; and

a second customer, ~~the~~ said second customer being a customer of the second participant, ~~the~~ said second customer maintaining a second-customer computer system,

~~the~~ said second-customer computer system comprising a Web server adapted to ~~serve Web pages~~ send an executable computer program to the first-customer computer system's browser, the method comprising the steps of:

invoking the signing interface;

retrieving data to be signed from a remote location;

determining whether to request a system service;

creating a service request for the system service;

transmitting the service request;

receiving a response to the service request;

forwarding the data to be signed to the signing module;

receiving a digital signature for the data to be signed from the signing module; and

forwarding the digital signature to a remote location specified by the ~~Web application~~ executable computer program.

46. (currently amended) The method of claim 43, further comprising~~:~~ the step of presenting to the first customer an option to request a system service.

47. (original) The method of claim 44, wherein the system service is a warranty.

48. (currently amended) The method of claim 45, wherein the response to the service request comprises a warranty, and ~~wherein~~ the warranty is forwarded with the digital signature to the remote location specified by the ~~Web application~~ executable computer program.